

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-281093

(43)Date of publication of application : 27.09.2002

(51)Int.Cl.

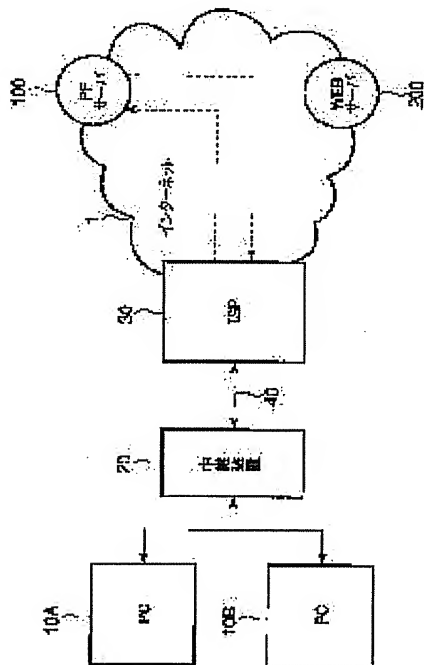
H04L 12/66

G06F 13/00

(21)Application number : 2001-078997 (71)Applicant : TOSHIBA CORP

(22)Date of filing : 19.03.2001 (72)Inventor : OKAMOTO KENICHI  
NAGAMI KENICHI

## (54) PROFILE DISTRIBUTION METHOD TO BE APPLIED TO NETWORK, AND NETWORK SYSTEM



(57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a method for allowing even a general user who lacks technical knowledge about a network to easily realize the packet filtering condition setting of a network repeater system based on profile information.

**SOLUTION:** This is a method for allowing a profile server 100 arranged on the Internet 1 to distribute the latest profile information to a network repeater system 20 by using an electronic mail function. The network repeater system 20 is allowed to periodically access to the profile server 100, and to acquire desired profile information as the attached file of the electronic

mail.

## CLAIMS

[Claim(s)]

[Claim 1]A profile distribution method characterized by comprising the following for distributing profile information required for a packet-filtering function from a server connected to a network to network equipment connected to the network concerned.

A step which connects said network equipment with a predetermined communications protocol to said server which manages said profile information.

A step which extracts and acquires desired profile information from profile information transmitted from said server.

[Claim 2]Said network equipment is network repeating installation which has a relay function of installed user terminals and a network, and said profile information is used for it, The profile distribution method according to claim 1 constituting so that a packet-filtering function to said installed user terminals may be realized.

[Claim 3]The profile distribution method according to claim 1 which said server is a mail server connected to the Internet, and is characterized by being constituted so that said profile information may be distributed by an electronic mail function which uses Internet Protocol.

[Claim 4]Said server distributes list information which presents profile information of a distribution object by an electronic mail function, The profile distribution method according to claim 1 constituting so that profile information by which the selection request was carried out from the list information concerned may be distributed as an attached file of an E-mail.

[Claim 5]Network repeating installation which has a relay function of installed user terminals and a network, comprising:

A means to access on condition of predetermined to a server which is connected to a network and manages profile information required for a packet-filtering function.

A means to extract and acquire desired profile information from profile information transmitted from said server, and a means to notify said acquired profile information to said installed user terminals.

[Claim 6]Said server is a mail server connected to the Internet, and said acquisition means, The network repeating installation according to claim 5 constituting so that said profile information distributed as an attached file of an E-mail by electronic mail function which uses Internet Protocol by said server may be acquired.

[Claim 7]Said server has a means to distribute list information which presents profile information of a distribution object by an electronic mail function, and receives said list information, The network repeating installation according to claim 5 or 6 having further a means to choose desired profile information from the list information concerned, and

to require of said server.

[Claim 8]A network system which distributes profile information required for a packet-filtering function to network equipment connected to the network concerned by a server connected to a network, comprising:

A means to accumulate the newest profile information.

A means to distribute said profile information to said network equipment with a predetermined communications protocol.

[Claim 9]The network system according to claim 8 which said server is a mail server connected to the Internet, and is characterized by being constituted so that said profile information may be distributed as an attached file of an E-mail by an electronic mail function which uses Internet Protocol.

[Claim 10]The network system according to claim 8 or 9, wherein said server is further provided with a means to distribute list information which presents profile information of a distribution object by an electronic mail function.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to the art of realizing the packet-filtering function for a general user's information protection especially, about the profile distribution method applied to networks, such as the Internet.

[0002]

[Description of the Prior Art]In recent years, the terminal equipment which can access alone at the Internet not only a personal computer (PC) but into a cellular phone, mobile information terminals (PDA:Personal Digital Assistant), etc. (connection) is developed. Such a terminal equipment has an Internet Protocol (IP) communication function, and enables offer of the network environment in a personal level via the Internet.

[0003]As PC10 and PDA11 are shown in drawing 6, access to the Internet 1 is attained via the line networks 40, such as the network repeating installation 60, such as a router, and ISDN, and Internet Service Provider (ISP) 30. ISP30 consists of WEB servers and is building what is called WWW (World Wide Web) with other WEB servers 200 connected to the Internet 1.

[0004]The security function for avoiding disclosure, destruction, etc. of personal information by the attack and unauthorized entry from the Internet in terminal equipments (it is named a user terminal generically below) linked to the Internet, such

as PC10 and PDA11, is important. The packet-filtering function for preventing the inaccurate packet (IP packet) from the Internet in this security function is common knowledge.

[0005]A packet-filtering function is a function (penetration determining function of a packet) which is provided, for example in the network repeating installation 60, such as a router, and controls the propriety of passage of a packet based on the IP header information on a packet, including IP address etc.

[0006]

[Problem(s) to be Solved by the Invention]As mentioned above, the newest packet-filtering function for protecting a user's information is provided in the network equipment linked to the Internet. However, since the art of the attack from the Internet aiming at disclosure, destruction, etc. of personal information is also rapid progress, in order to cope with a new attack, renewal of a packet-filtering function is indispensable.

[0007]Roughly, as shown in drawing 7, a packet-filtering function here, It is the function to judge the propriety of passage of the packets (e-mail, WWW, FTP, etc.) transmitted from certain PC10A with the network repeating installation 60, such as a router, and to perform a penetration (relay) or interception (abandonment) of the packet concerned. The network repeating installation 60 controls a penetration or interception of a packet based on the IP address (a transmission source address and transmission destination address) included in the IP header information on a packet.

[0008]In recent years, the network repeating installation 60 has realized the packet-filtering function using the profile information which summarized as a definition file what described the definition for every various packets as determination information (filtering conditioning information) for judging the propriety of passage of a packet. Various kinds of methods are proposed as a method of creating this profile information (see JP,9-233113,A).

[0009]As mentioned above, in order to update a packet-filtering function, it is necessary to update profile information and to change the packet-filtering conditioning of the network repeating installation 60. However, the updating operation concerned is complicated and it is difficult for a general user deficient in a network know how.

[0010]Then, even if the purpose of this invention is a general user deficient in a network know how, there is in providing how the packet-filtering conditioning of network repeating installation is easily realizable based on profile information.

[0011]

[Means for Solving the Problem]Especially this invention relates to a way packet-filtering conditioning of network repeating installation (for example, router) to

which each user terminal is connected is easily realizable, about a distribution method of profile information which used an electronic mail function on the Internet.

[0012]Specifically, the 1st viewpoint of this invention is a profile distribution method for distributing profile information required for a packet-filtering function from a server connected to networks, such as the Internet, to network repeating installation connected to the network concerned. Network repeating installation receives profile information from a server by an electronic mail function, and extracts and acquires desired profile information.

[0013]With such composition, the network repeating installation can access a server (a profile server or a mail server) which provides profile information periodically, for example, and can acquire the newest profile information by an electronic mail function. And the network repeating installation can change packet-filtering conditioning by setting up desired profile information according to directions from a user eventually. If it puts in another way, network repeating installation will become possible [ updating a packet-filtering function almost automatically ].

[0014]The 2nd viewpoint of this invention functions as a mail server connected to the Internet, and is related with a server which distributes profile information to network repeating installation on the Internet as an attached file of an E-mail by an electronic mail function.

[0015]With such composition, the Internet business model which realizes a kind of Internet Service Provider (ISP) who manages a profile server which distributes profile information can be provided. That is, service operations of special ISP which prepares profile information which specifies a packet-filtering function for every applications of various kinds of, for example, and provides it by E-mail to network repeating installation of demand-demanded profile information origin, or general ISP are realizable.

[0016]

[Embodiment of the Invention]With reference to drawings, an embodiment of the invention is described below.

[0017](System configuration) Drawing 1 is a block diagram showing the important section of the network system related to this embodiment.

[0018]According to the embodiment, PC(they may be two sets for convenience) 10A which is tens of sets of user terminals, for example, and 10B assume the system connected to the network repeating installation (specifically router etc.) 20. As a user terminal, not only PC but portable terminal equipment, such as a cellular phone and PDA, is contained. As for the Internet repeating installation 20, access to the Internet 1

is attained, for example via the line network 40 and Internet Service Providers (ISP) 30, such as ISDN. ISP30 consists of WEB servers and is building WWW (World Wide Web) with other WEB servers 200 connected to the Internet 1.

[0019]Here, in the embodiment, the mail server called the profile (PF) server 100 for convenience is formed on the Internet 1. The PF server 100 performs processing which distributes the profile information for performing filtering conditioning in a packet-filtering function using an electronic mail function so that it may mention later.

[0020](Profile information) As profile information was mentioned above, the network repeating installation 20 summarizes as a definition file what described the definition for every various packets as determination information (filtering conditioning information) for judging the propriety of passage of a packet. Profile information consists of information which directs IN/OUT of transmitting agency and address (transmission destination) IP address, and transmitting origin and a destination port number (range), a protocol, filter operation (a penetration or interception), and a packet, as specifically shown in drawing 2. A transmitting agency and destination IP addresses mean the application which a user uses so that the packet which is the target of filtering (a penetration or interception) may be specified and mentioned later. A port number and a protocol (here TCP) are the information for controlling communication of specific application. Here, the port number to be used may not restrict application in one, but two or more continuous port numbers may be used for it. In the network repeating installation 20 of the embodiment, a LAN side port and the WAN side port (Internet side port) are provided. In this case, setting out of a port number enables it to control communication of an IP packet to each of a LAN side port and the WAN side port.

[0021]The profile information shown in drawing 2 is a definition file in the case of performing conditioning of two or more IP packet filtering, for example, is a TCP (Transmission Control Protocol) protocol, It is the information for making the packet of the application (A) which uses No. 4000, No. 5000, and No. 6000 simultaneously as a port number penetrate (passage). If it puts in another way, when the network repeating installation 20 sets up the profile information concerned, PC10A and 10B become possible [ using application (A) ], and can access the information by application (A) on the Internet 1.

[0022]Here, in the former, as an IP packet is shown in drawing 5, the header information which consists of IP header structure is established. According to a protocol, the header information which consists of TCP header structure corresponding to a TCP protocol and UDP header structure corresponding to an UDP (User Datagram Protocol) protocol is included.

[0023](Profile distribution method) With reference to the flow chart of drawing 3 and drawing 4, the profile distribution method of the embodiment is explained from drawing 1 below.

[0024]The network repeating installation 20 of the embodiment is periodical, or according to the directions from a user, the PF server 100 on the Internet 1 is accessed, and it acquires an E-mail (Step S1). The PF server 100 is a mail server which special ISP is managing, for example, and transmits PF list mail with what is called an e-mail service function. Here, the PF server 100 transmits the attached file of the mail which performed user authentication processing by the password and user ID which were enciphered as well as the usual electronic mail function, and was encoded for example, in BASE64 form.

[0025]As PF list mail is specifically shown in drawing 3 (A), a profile name, a login ID, a password, a use (here, the application A, B, and C specifies), etc. are described. The network repeating installation 20 shifts to the processing which acquires the file information concerned, when new profile information other than the existing profile information is registered from acquired PF list mail (YES of Step S2).

[0026]The network repeating installation 20 reads a login ID and a password in acquired PF list mail, and logs in to the PF server 100 with the login ID concerned and a password (step S4). Then, the network repeating installation 20 downloads the E-mail transmitted from the PF server 100 concerned by checking the transmitting mail addressed to the user ID concerned from the PF server 100 (YES of Step S5). In not receiving an E-mail, it performs predetermined error handling (Step S7).

[0027]The PF server 100 transmits the E-mail which has the profile information corresponding to the application (A) demanded from the network repeating installation 20 as an attached file, as shown, for example in drawing 3 (B). The network repeating installation 20 develops the attached file of the downloaded E-mail, and the profile information (see drawing 2) corresponding to application (A) is extracted here (Step S6).

[0028]Here, the user can check the profile information acquired from the network repeating installation 20, for example on a homepage by operating PC10A and 10B. It is determined whether the network repeating installation 20 applies the acquired profile information to a packet-filtering function according to the directions from a user.

[0029]If it is a profile distribution method of the embodiment as mentioned above, the network repeating installation 20 connected to each user terminal, It is the newest profile information and the definition file which makes possible conditioning of two or more IP packet filtering can be acquired from the PF server 100 on the Internet 1 by the usual electronic mail function. Therefore, the user can realize easily conditioning of IP

packet filtering for using desired application (A), without doing special work. Thereby, especially the user using the Internet can update a packet-filtering function easily, without requiring the special knowledge about a network.

[0030] If it puts in another way and will be a profile distribution method of the embodiment, the Internet business model which realizes a kind of Internet Service Provider (ISP) who manages the profile server which distributes profile information can be provided. Namely, the profile information which realizes the packet-filtering function which regulates the communication function for every applications of various kinds of, for example is prepared, The service operations of special ISP which provides the demanded profile information by E-mail to the network repeating installation of a requiring agency, or general ISP are realizable.

[0031]

[Effect of the Invention] As explained in full detail above, according to this invention, the newest profile information for realizing a packet-filtering function is acquirable from networks, such as the Internet, using a usual communications protocol like an electronic mail function. Therefore, even if it is a general user deficient in a network know how, based on profile information, the packet-filtering conditioning of network repeating installation is easily realizable.

---

## DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]

[Drawing 1] The block diagram showing the important section of the network system about the embodiment of this invention.

[Drawing 2] The figure showing an example of the file information about the embodiment.

[Drawing 3] The figure for explaining the contents of e-mail in the profile distribution method about the embodiment.

[Drawing 4] The flow chart for explaining the procedure of the profile distribution method about the embodiment.

[Drawing 5] The figure for explaining the contents of the IP header information on the conventional packet.

[Drawing 6] The block diagram for explaining the network system in the conventional Internet.

[Drawing 7] The figure for explaining the conventional packet-filtering function.

[Description of Notations]

1 -- Internet  
10A, 10B -- Personal computer (PC)  
11 -- PDA  
20, 60 -- Network repeating installation  
30 -- Internet Service Provider (ISP)  
40 -- Line network  
100 -- Profile (PF) server  
200 -- WEB server

---

**\* NOTICES \***

**JPO and INPIT are not responsible for any  
damages caused by the use of this translation.**

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

(19) 日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11) 特許出願公開番号  
特開2002-281093  
(P2002-281093A)

(43) 公開日 平成14年9月27日 (2002.9.27)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード* (参考)
H 0 4 L 12/66		H 0 4 L 12/66	B 5 B 0 8 9
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 Z 5 K 0 3 0

審査請求 未請求 請求項の数10 O L (全 6 頁)

(21) 出願番号 特願2001-78997(P2001-78997)

(22) 出願日 平成13年3月19日 (2001.3.19)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 岡本 謙一

東京都府中市東芝町1番地 株式会社東芝  
府中事業所内

(72) 発明者 永見 健一

東京都府中市東芝町1番地 株式会社東芝  
府中事業所内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

Fターム(参考) 5B089 GA12 GA21 GB01 GB02 HA10  
JA31 JB22

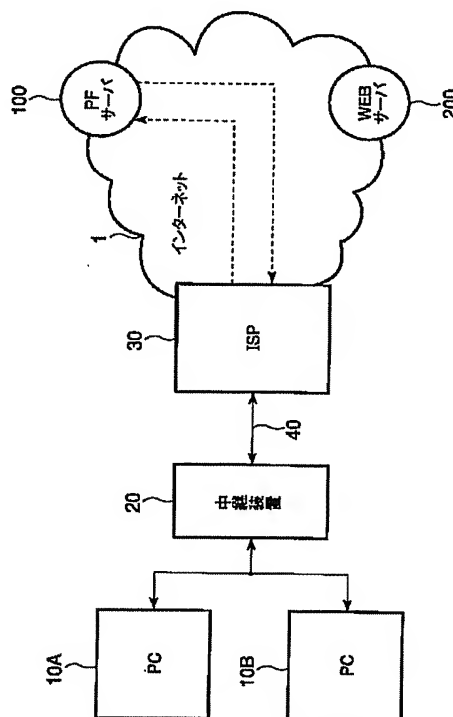
5K030 GA15 HD03 HD06 LC01

(54) 【発明の名称】 ネットワークに適用するプロファイル配信方法及びネットワークシステム

(57) 【要約】

【課題】 ネットワークの専門知識に乏しい一般ユーザであっても、プロファイル情報に基づいてネットワーク中継装置の packet フィルタリング条件設定を容易に実現できる方法を提供することにある。

【解決手段】 インターネット 1 上に設けられたプロファイルサーバ 100 により、電子メール機能を利用して、最新のプロファイル情報をネットワーク中継装置 20 に配信する方法が開示されている。ネットワーク中継装置 20 は、定期的にプロファイルサーバ 100 にアクセスし、所望のプロファイル情報を電子メールの添付ファイルとして取得することができる。



## 【特許請求の範囲】

【請求項 1】 ネットワークに接続されたサーバから、パケットフィルタリング機能に必要なプロファイル情報を当該ネットワークに接続されたネットワーク機器に対して配信するためのプロファイル配信方法であって、前記ネットワーク機器は、前記プロファイル情報を管理する前記サーバに対して所定の通信プロトコルにより接続するステップと、前記サーバから送信されるプロファイル情報から所望のプロファイル情報を抽出して取得するステップと、からなるプロファイル配信方法。

【請求項 2】 前記ネットワーク機器は、ユーザ端末装置とネットワークとの中継機能を有するネットワーク中継装置であり、前記プロファイル情報を使用して、前記ユーザ端末装置に対するパケットフィルタリング機能を実現するように構成されていることを特徴とする請求項 1 記載のプロファイル配信方法。

【請求項 3】 前記サーバは、インターネットに接続されたメールサーバであり、インターネットプロトコルを使用した電子メール機能により前記プロファイル情報を配信するように構成されていることを特徴とする請求項 1 記載のプロファイル配信方法。

【請求項 4】 前記サーバは、配信対象のプロファイル情報を提示するリスト情報を電子メール機能により配信し、当該リスト情報から選択要求されたプロファイル情報を電子メールの添付ファイルとして配信するように構成されていることを特徴とする請求項 1 記載のプロファイル配信方法。

【請求項 5】 ユーザ端末装置とネットワークとの中継機能を有するネットワーク中継装置であって、ネットワークに接続されて、パケットフィルタリング機能に必要なプロファイル情報を管理するサーバに対して、所定の条件でアクセスする手段と、前記サーバから送信されるプロファイル情報から所望のプロファイル情報を抽出して取得する手段と、前記取得したプロファイル情報を前記ユーザ端末装置に対して通知する手段と、を具備したことを特徴とするネットワーク中継装置。

【請求項 6】 前記サーバはインターネットに接続されたメールサーバであり、前記取得手段は、前記サーバによりインターネットプロトコルを使用した電子メール機能により電子メールの添付ファイルとして配信された前記プロファイル情報を取得するように構成されていることを特徴とする請求項 5 記載のネットワーク中継装置。

【請求項 7】 前記サーバは、配信対象のプロファイル情報を提示するリスト情報を電子メール機能で配信する

手段を有し、

前記リスト情報を受信して、当該リスト情報から所望のプロファイル情報を選択して前記サーバに要求する手段をさらに備えていることを特徴とする請求項 5 または請求項 6 記載のネットワーク中継装置。

【請求項 8】 ネットワークに接続されたサーバにより、パケットフィルタリング機能に必要なプロファイル情報を当該ネットワークに接続されたネットワーク機器に対して配信するネットワークシステムであって、

最新のプロファイル情報を蓄積する手段と、前記プロファイル情報を所定の通信プロトコルで前記ネットワーク機器に対して配信する手段と、を具備したことを特徴とするネットワークシステム。

【請求項 9】 前記サーバはインターネットに接続されたメールサーバであり、インターネットプロトコルを使用した電子メール機能により電子メールの添付ファイルとして前記プロファイル情報を配信するように構成されていることを特徴とする請求項 8 記載のネットワークシステム。

【請求項 10】 前記サーバは、配信対象のプロファイル情報を提示するリスト情報を電子メール機能により配信する手段をさらに備えていることを特徴とする請求項 8 または請求項 9 記載のネットワークシステム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、インターネットなどのネットワークに適用するプロファイル配信方法に関し、特に一般ユーザの情報保護のためのパケットフィルタリング機能を実現する技術に関する。

## 【0002】

【従来の技術】近年、パーソナルコンピュータ（PC）だけでなく、携帯電話やモバイル情報端末（PDA: Personal Digital Assistant）などの中にも、単体でインターネットにアクセス（接続）できる端末機器が開発されている。このような端末機器は、インターネットプロトコル（IP）通信機能を有し、インターネットを介して個人レベルでのネットワーク環境の提供を可能にしている。

【0003】PC10やPDA11は、図6に示すように、ルータなどのネットワーク中継装置60、ISDNなどの回線網40、及びインターネットサービスプロバイダ（ISP）30を経由して、インターネット1へのアクセスが可能になっている。ISP30はWEBサーバからなり、インターネット1に接続されている他のWEBサーバ200と共に、いわゆるWWW（World Wide Web）を構築している。

【0004】インターネットに接続するPC10やPDA11などの端末機器（以下ユーザ端末と総称する）では、インターネットからのアタックや不正侵入により個人情報の漏洩や破壊などを回避するためのセキュリティ

10

20

30

40

50

機能が重要である。このセキュリティ機能には、インターネットからの不正なパケット（IPパケット）を阻止するためのパケットフィルタリング機能が周知である。

【0005】パケットフィルタリング機能は、例えばルータなどのネットワーク中継装置60に設けられて、パケットのIPヘッダ情報（IPアドレスなど）に基づいてパケットの通過の可否を制御する機能（パケットの透過判定機能）である。

【0006】

【発明が解決しようとする課題】前述したように、インターネットに接続するネットワーク機器には、ユーザの情報を保護するための最新のパケットフィルタリング機能が設けられている。しかし、個人情報の漏洩や破壊などを目的としたインターネットからの攻撃の技術も日進月歩であるため、新たな攻撃に対処するためにパケットフィルタリング機能の更新が必要不可欠である。

【0007】ここで、パケットフィルタリング機能は、概略的には図7に示すように、あるPC10Aから送信されるパケット（メール、WWW、FTPなど）を、ルータなどのネットワーク中継装置60により通過の可否を判定し、当該パケットの透過（中継）又は遮断（廃棄）を実行する機能である。ネットワーク中継装置60は、パケットのIPヘッダ情報に含まれるIPアドレス（送信元アドレス及び送信先アドレス）に基づいてパケットの透過又は遮断を制御する。

【0008】近年では、ネットワーク中継装置60は、パケットの通過の可否を判定するための判定情報（フィルタリング条件設定情報）として、各種パケット毎に定義を記述したものを定義ファイルとして纏めたプロファイル情報を使用してパケットフィルタリング機能を実現している。このプロファイル情報を作成する方法としては、各種の方法が提案されている（例えば特開平9-233113号公報を参照）。

【0009】前述したように、パケットフィルタリング機能を更新するには、プロファイル情報を更新してネットワーク中継装置60のパケットフィルタリング条件設定を変更する必要がある。しかしながら、当該更新作業は複雑であり、ネットワークの専門知識に乏しい一般ユーザには困難である。

【0010】そこで、本発明の目的は、ネットワークの専門知識に乏しい一般ユーザであっても、プロファイル情報に基づいてネットワーク中継装置のパケットフィルタリング条件設定を容易に実現できる方法を提供することにある。

【0011】

【課題を解決するための手段】本発明は、特にインターネット上において、電子メール機能を利用したプロファイル情報の配信方法に関し、各ユーザ端末が接続されているネットワーク中継装置（例えばルータ）のパケット

フィルタリング条件設定を容易に実現できる方法に関する。

【0012】具体的には、本発明の第1の観点は、インターネットなどのネットワークに接続されたサーバから、パケットフィルタリング機能に必要なプロファイル情報を当該ネットワークに接続されたネットワーク中継装置に対して配信するためのプロファイル配信方法である。ネットワーク中継装置は、プロファイル情報を例えば電子メール機能によりサーバから受信し、所望のプロファイル情報を抽出して取得する。

【0013】このような構成であれば、ネットワーク中継装置は、例えば定期的にプロファイル情報を提供するサーバ（プロファイルサーバ又はメールサーバ）にアクセスし、最新のプロファイル情報を電子メール機能により取得することができる。そして、ネットワーク中継装置は、最終的にはユーザからの指示に応じて、所望のプロファイル情報を設定することにより、パケットフィルタリング条件設定を変更できる。換言すれば、ネットワーク中継装置は、ほぼ自動的にパケットフィルタリング機能を更新することが可能となる。

【0014】本発明の第2の観点は、インターネットに接続されたメールサーバとして機能し、電子メール機能により電子メールの添付ファイルとしてプロファイル情報をインターネット上のネットワーク中継装置に配信するサーバに関する。

【0015】このような構成であれば、プロファイル情報を配信するプロファイルサーバを運営する一種のインターネットサービスプロバイダ（ISP）を実現するインターネットビジネスモデルを提供できる。即ち、例えば各種のアプリケーション毎のパケットフィルタリング機能を規定するプロファイル情報を用意し、要求されたプロファイル情報を要求元のネットワーク中継装置に対して電子メールで提供する専門ISPまたは一般ISPのサービス業務を実現できる。

【0016】

【発明の実施の形態】以下図面を参照して、本発明の実施の形態を説明する。

【0017】（システム構成）図1は、本実施形態に係るネットワークシステムの要部を示すブロック図である。

【0018】同実施形態では、例えば数十台のユーザ端末であるPC（便宜的に2台とする）10A、10Bが、ネットワーク中継装置（具体的にはルータなど）20に接続されたシステムを想定する。なお、ユーザ端末としては、PCだけでなく、携帯電話やPDAなどの携帯端末機器も含まれる。インターネット中継装置20は、例えばISDNなどの回線網40及びインターネットサービスプロバイダ（ISP）30を経由して、インターネット1へのアクセスが可能になっている。ISP30はWEBサーバからなり、インターネット1に接続

10

20

30

40

50

されている他のWEBサーバ200と共に、WWW (World Wide Web) を構築している。

【0019】ここで、同実施形態では、インターネット1上には、便宜的にプロファイル(PF)サーバ100と呼ぶメールサーバが設けられている。PFサーバ100は、後述するように、パケットフィルタリング機能でのフィルタリング条件設定を行うためのプロファイル情報を、電子メール機能を使用して配信する処理を実行する。

【0020】(プロファイル情報) プロファイル情報は、前述したように、ネットワーク中継装置20は、パケットの通過の可否を判定するための判定情報(フィルタリング条件設定情報)として、各種パケット毎に定義を記述したものを定義ファイルとして纏めたものである。プロファイル情報は、具体的には図2に示すように、送信元及び宛先(送信先)IPアドレス、送信元及び宛先ポート番号(範囲)、プロトコル、フィルタ動作(透過又は遮断)及びパケットのIN/OUTを指示する情報からなる。送信元及び宛先IPアドレスは、フィルタリング(透過又は遮断)の対象となるパケットを特定し、後述するように、例えばユーザが使用するアプリケーションを意味する。ポート番号及びプロトコル(ここではTCP)は、特定アプリケーションの通信を制御するための情報である。ここで、アプリケーションは、使用するポート番号が1つとは限らず、連続する複数のポート番号を使用する場合もある。同実施形態のネットワーク中継装置20では、LAN側ポートとWAN側ポート(インターネット側ポート)が設けられる。この場合、ポート番号の設定により、LAN側ポートとWAN側ポートのそれぞれに対して、IPパケットの通信を制御することが可能となる。

【0021】図2に示すプロファイル情報は、複数のIPパケットフィルタリングの条件設定を行う場合の定義ファイルであり、例えばTCP(Transmission Control Protocol)プロトコルで、ポート番号として4000番、5000番、6000番を同時に使用するアプリケーション(A)のパケットを透過(通過)させるための情報である。換言すれば、ネットワーク中継装置20が当該プロファイル情報を設定することにより、PC10A、10Bはアプリケーション(A)を使用することが可能となり、インターネット1でアプリケーション(A)による情報のアクセスを行うことができる。

【0022】ここで、従来では、IPパケットは、図5に示すように、IPヘッダ構造からなるヘッダ情報が設けられている。また、プロトコルに従って、TCPプロトコルに対応するTCPヘッダ構造や、UDP(User Datagram Protocol)プロトコルに対応するUDPヘッダ構造からなるヘッダ情報が含まれる。

【0023】(プロファイル配信方法) 以下図1から図3及び図4のフローチャートを参照して、同実施形態の

プロファイル配信方法を説明する。

【0024】同実施形態のネットワーク中継装置20は、定期的またはユーザからの指示に応じて、インターネット1上のPFサーバ100にアクセスし、電子メールを取得する(ステップS1)。PFサーバ100は、例えば専門ISPが運営しているメールサーバであり、いわゆる電子メールサービス機能によりPFリストメールを送信する。ここで、PFサーバ100は、通常の電子メール機能と同様に、暗号化されたパスワードやユーザIDによるユーザ認証処理を実行し、また例えばBASE64形式でエンコードされたメールの添付ファイルを送信する。

【0025】PFリストメールは、具体的には図3(A)に示すように、プロファイル名、ログインID、パスワード、及び用途(ここではアプリケーションA、B、Cの指定)などが記述されている。ネットワーク中継装置20は、取得したPFリストメールから、既存のプロファイル情報以外の新しいプロファイル情報が登録されている場合に、当該ファイル情報を取得する処理に移行する(ステップS2のYES)。

【0026】ネットワーク中継装置20は、取得したPFリストメールからログインID、パスワードを読み取り、当該ログインID、パスワードによりPFサーバ100にログインする(ステップS4)。この後、ネットワーク中継装置20は、PFサーバ100から当該ユーザID宛のメール送信を確認することにより、当該PFサーバ100から送信される電子メールをダウンロードする(ステップS5のYES)。なお、電子メールを受信しない場合には、所定のエラー処理を実行する(ステップS7)。

【0027】PFサーバ100は、例えば図3(B)に示すように、ネットワーク中継装置20から要求されたアプリケーション(A)に対応するプロファイル情報を添付ファイルとして有する電子メールを送信する。ネットワーク中継装置20は、ダウンロードした電子メールの添付ファイルを展開し、ここではアプリケーション(A)に対応するプロファイル情報(図2を参照)を抽出する(ステップS6)。

【0028】ここで、ユーザはPC10A、10Bを操作することにより、ネットワーク中継装置20から取得したプロファイル情報を、例えばホームページ上で確認することができる。ネットワーク中継装置20は、ユーザからの指示に応じて、取得したプロファイル情報をパケットフィルタリング機能に適用するか否かを決定する。

【0029】以上のように同実施形態のプロファイル配信方法であれば、各ユーザ端末に接続されたネットワーク中継装置20は、インターネット1上のPFサーバ100から、最新のプロファイル情報であり、複数のIPパケットフィルタリングの条件設定を可能とする定義フ

ファイルを通常の電子メール機能で取得することができる。従って、ユーザは特別な作業を行うことなく、所望のアプリケーション（Ａ）を利用するためのＩＰパケットフィルタリングの条件設定を容易に実現することができる。これにより、インターネットを利用するユーザは、特にネットワークに関する専門的な知識を要することなく、パケットフィルタリング機能の更新を容易に行うことができる。

【0030】換言すれば、同実施形態のプロファイル配信方法であれば、プロファイル情報を配信するプロファイルサーバを運営する一種のインターネットサービスプロバイダ（ISP）を実現するインターネットビジネスモデルを提供できる。即ち、例えば各種のアプリケーション毎の通信機能を規制するパケットフィルタリング機能を実現するプロファイル情報を用意し、要求されたプロファイル情報を要求元のネットワーク中継装置に対して電子メールで提供する専門ISPまたは一般ISPのサービス業務を実現できる。

【0 0 3 1】

【発明の効果】以上詳述したように本発明によれば、インターネットなどのネットワークから電子メール機能のような通常の通信プロトコルを利用して、パケットフィルタリング機能を実現するための最新のプロファイル情報を取得できる。従って、ネットワークの専門知識に乏しい一般ユーザであっても、プロファイル情報に基づいてネットワーク中継装置のパケットフィルタリング条件＊

\* 設定を容易に実現することができる。

【図面の簡単な説明】

【図 1】本発明の実施形態に関するネットワークシステムの要部を示すブロック図。

【図2】同実施形態に関するファイル情報の一例を示す図。

【図3】同実施形態に関するプロフィール配信方法でのメール内容を説明するための図。

【図4】同実施形態に関するプロファイル配信方法の手順を説明するためのフローチャート。

【図 5】従来のパケットの IP ヘッダ情報の内容を説明するための図。

【図6】従来のインターネットでのネットワークシステムを説明するためのブロック図。

【図7】従来のパケットフィルタリング機能を説明するための図。

【符号の説明】

1…インターネット

10A, 10B…パーソナルコンピュータ (PC)

1 1 ... P D A

20, 60…ネットワーク中継装置

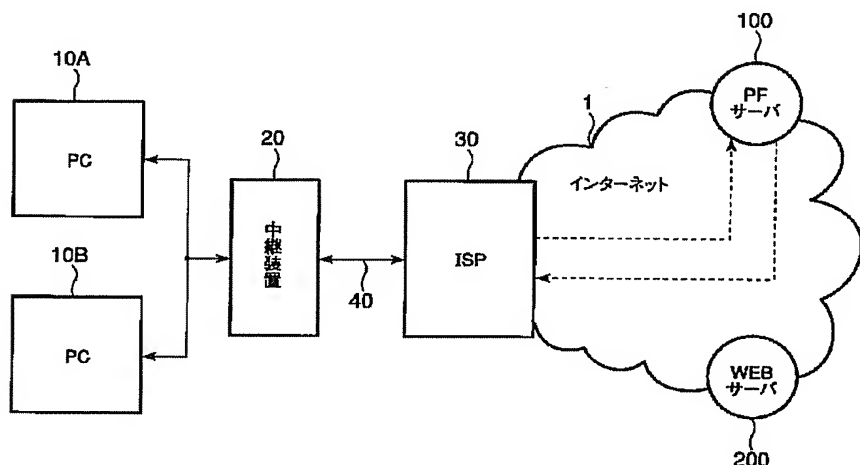
30…インターネットサービスプロバイダ（ISP）

40...回線網

100…プロフィール (PF) サーバ

200...WEBサーバ

【义 1】



【图 3】

ブロードファイルリストメール

```
Subject : Profile List
Profile1 : "アブリケーションA"
Login1 : "abcdcf"
Password1 : "hkk/21kg+ht"
Profile2 : "アブリケーションB"
Login2 : "ghijklmn"
Password2 : "fasdfahkald"
Profile3 : "アブリケーションC"
Login3 : "opqrstu"
Password3 : "tyqo75a1adba"
:
```

(A)

【图 2】

送信元IPアドレス		宛先IPアドレス		送信元ポート番号 (範囲)		宛先ポート番号(範囲)		プロトコル	動作	IN/OUT
*	*	*	*	4000	4000	*	*	TCP	透過	IN
*	*	*	*	5000	5000	*	*	TCP	透過	IN
*	*	*	*	6000	6000	*	*	TCP	透過	IN

(B)

Subject : アプリケーションA

用途：アプリケーションAを使用するためのプロファイルです。  
以下、添付ファイル

[illegible]

